DOWNLOAD PDF WHAT REGULATIONS ARE NEEDED TO ENSURE AIR SECURITY?

Chapter 1 : Whatâ€™s needed to ensure safety and security in UAV software - Military Embedded System

We will hear from an expert in air security and other witnesses representing the airlines, airports, pilots, flight attendants, and consumers about what regulations are needed to ensure air secu-.

What security responsibilities does an IAC have based on published regulations? Among other things, an IAC must: Ensure that its employees and agents e. Refer to 49 CFR Protect what the TSA has defined as Sensitive Security Information "SSI" from disclosure to individuals who do not have a need-to-know of such information in order to perform security-related job responsibilities. Ensure that its employees and agents AR personnel have been trained in their particular security responsibilities so they will be able to properly perform such responsibilities. This training must be repeated annually. The directly-regulated parties under TSA air cargo security regulations are air carriers airlines , forwarders indirect air carriers and airport operators. As a trucker, you fall under TSA security regulations when you are hired by one of these regulated parties as a sub-contractor to transport or otherwise handle air cargo. In particular, when a forwarder hires you, the requirement for a Security Threat Assessment "STA" and training become applicable. How do truck drivers and other trucking company personnel with unescorted access to cargo apply for a Security Threat Assessment "STA"? This must be done through an IAC air forwarder. Each driver must complete and sign a detailed paper applicable form. A trucking company needs to work with an IAC to obtain this form and subsequently submit the information to the TSA for processing. What does this training for drivers and other sub-contracted personnel consist of and how long does it take? The subject matter to be trained is specified in 49 CFR As is typically the case, the training consists of a presentation of the information to be learned by an instructor or other means, followed by an assessment which a person must pass to complete the training. The required training and assessment for a truck driver will typically require hours, depending on the method of delivery and a persons existing understanding of the subject matter. Annual refresher training will typically take less time. As a trucking company, how can we obtain this training for our drivers and other personnel who have air cargo security responsibilities? In general, this training must also be obtained or arranged for through an IAC air forwarder. There are several different methods of training delivery: An IAC can directly conduct training for its truckers and other agents. An IAC can provide needed training and assessment materials to a trucking company or other agent, from which training and assessment can be conducted by such company with results reported back to the IAC. An IAC can authorize a third-party training provider, acting on its behalf as agent authorized representative for training , to train and assess your company personnel. How does the training work? GISTnet training is taken online, on demand, and can be accessed from any web connection. The courses are self paced and can be paused and resumed as necessary. Audio narration is also provided for users who prefer to listen to the material rather than read the lesson text. Throughout the lessons, users are presented with relevant questions to reinforce the learning process. At the end of each lesson the learner must pass an assessment in order to complete the assignment. The learner can take the assessment as many times as necessary to pass at no additional charge. How does GISTnet go about training trucking company personnel? An IAC any IAC must authorize us to make our security training available to a trucking company or other agent through a simple on-line process. We will then work with a designated person at the company to be trained to assign their personnel to the training. Our system provides progress tracking and reminder notifications to help ensure assigned training is promptly completed, and further provides reminders when annual refresher training is due for each person. Upon completion of the training, a paper certificate may be printed out for presentation to the trained person. What does GISTnet charge for training trucking company personnel? If we can get the needed training and assessment materials from an IAC without charge, why should our company pay GISTnet to provide the training? Training materials alone do not constitute training, and training is never "free. By automating the training, all these steps, plus the needed record-keeping, are combined into a process that:

DOWNLOAD PDF WHAT REGULATIONS ARE NEEDED TO ENSURE AIR SECURITY?

Chapter 2 : Cyber-security regulation - Wikipedia

Full text of "WHAT REGULATIONS ARE NEEDED TO ENSURE AIR SECURITY?" See other formats.

Background[edit] In the DoD released a guidance called the Department of Defense Strategy for Operating in Cyberspace which articulated five goals: As of systems protecting critical infrastructure, called cyber critical infrastructure protection of cyber CIP have also been included. The three regulations mandate that healthcare organizations, financial institutions and federal agencies should protect their systems and information. The vague language of these regulations leaves much room for interpretation. The idea has not been fully vetted and would require additional legal analysis before a rulemaking could begin. In , California passed the Notice of Security Breach Act, which requires that any company that maintains personal information of California citizens and has a security breach must disclose the details of the event. Also, the regulation creates an incentive for companies to voluntarily invest in cybersecurity to avoid the potential loss of reputation and the resulting economic loss that can come from a successful cyber attack. The regulation dictates for businesses to maintain a reasonable level of security and that they required security practices also extend to business partners. However, like the federal legislation, it requires a "reasonable" level of cybersecurity, which leaves much room for interpretation until case law is established. Congressmen have also proposed "expanding Gramm-Leach-Bliley to all industries that touch consumer financial information, including any firm that accepts payment by a credit card. The Information Protection and Security Act requires that data brokers "ensure data accuracy and confidentiality, authenticate and track users, detect and prevent unauthorized activity, and mitigate potential harm to individuals. A year of public debate and Congress hearings followed, resulting in the House of Representative passing an information sharing bill and the Senate developing a compromise bill seeking to balance national security, privacy, and business interests. Brennan , the chief counterterrorism adviser to the White House. It represents the latest iteration of policy but is not considered to be law as it has not been addressed by Congress yet. It seeks to improve existing public-private partnerships by enhancing timeliness of information flow between DHS and critical infrastructure companies. It directs federal agencies to share cyber threat intelligence warnings to any private sector entity identified as a target. It also tasks DHS with improving the process to expedite security clearance processes for applicable public and private sector entities to enable the federal government to share this information at the appropriate sensitive and classified levels. It directs the development of a framework to reduce cyber risks, incorporating current industry best practices and voluntary standards. Lastly, it tasks the federal agencies involved with incorporating privacy and civil liberties protections in line with Fair Information Practice Principles. The proposal was made in an effort to prepare the US from the expanding number of cyber crimes. In the proposal, Obama outlined three main efforts to work towards a more secure cyberspace for the US. The first main effort emphasized the importance of enabling cybersecurity information sharing. By enabling that, the proposal encouraged information sharing between the government and the private sector. That would allow the government to know what main cyber threats private firms are facing and would then allow the government to provide liability protection to those firms that shared their information. Furthermore, that would give the government a better idea of what the US needs to be protected against. Another main effort that was emphasized in this proposal was to modernize the law enforcement authorities to make them more equipped to properly deal with cyber crimes by giving them the tools they need in order to do so. It would also update classifications of cyber crimes and consequences. One way this would be done would be by making it a crime for overseas selling of financial information. Another goal of the effort is to place cyber crimes prosecutable. The last major effort of the legislative proposal was to require businesses to report data breaching to consumers if their personal information had been sacrificed. By requiring companies to do so, consumers are aware of when they are in danger of identity theft. The plan was made to create long-term actions and strategies in an effort to protect the US against cyber threats. The focus of the plan was to inform the public

about the growing threat of cyber crimes, improve cybersecurity protections, protects personal information of Americans, and to inform Americans on how to control digital security. One of the highlights of this plan include creating a "Commission on Enhancing National Cybersecurity. The second highlight of the plan is to change Government IT. The third highlight of the plan is to give Americans knowledge on how they can secure their online accounts and avoid theft of their personal information through multi-factor authentication. In the United States, the US Congress is trying to make information more transparent after the Cyber Security Act of , which would have created voluntary standards for protecting vital infrastructure, failed to pass through the Senate. It is not sufficient to merely put cyber security as a part of the IT Act. We have to see cyber security not only from the sectoral perspective, but also from the national perspective. To maximize their profits, corporations leverage technology by running most of their operations by the internet. Since there are a large number of risks that entail internetwork operations, such operations must be protected by comprehensive and extensive regulations. Existing cybersecurity regulations all cover different aspects of business operations and often vary by region or country in which a business operates. While US standards provide a basis for operations, the European Union has created a more tailored regulation for businesses operating specifically within the EU. Also, in light of Brexit , it is important to consider how the UK has chosen to adhere to such security regulations. The focus of their operations are on three factors: Recommendations to member states on the course of action for security breaches Policy making and implementation support for all members states of the EU Direct support with ENISA taking a hands-on approach to working with operational teams in the EU [13] ENISA is made up of a management board that relies on the support of the executive director and the Permanent Stakeholders Group. Most operations, however, are run by the heads of various departments. Operators of essential services include any organizations whose operations would be greatly affected in the case of a security breach if they engage in critical societal or economic activities. Such resources are given the responsibility of handling cybersecurity breaches in a way that minimizes impact. In addition, all member states of the EU are encouraged to share cyber security information. Both DSP and OES must provide information that allows for an in depth assessment of their information systems and security policies. Significant cybersecurity incidents are determined by the number of users affected by the security breach as well as the longevity of the incident and the geographical reach of the incident. Changes include the redefining of geographical borders. It applies to entities that operate in the EU or deal with the data of any resident of the EU. Consent plays a major role in the GDPR. Companies that hold data in regards to EU citizens must now also offer to them the right to back out of sharing data just as easily as when they consented to sharing data. Reactions[edit] While experts agree that cybersecurity improvements are necessary, there is disagreement about whether the solution is more government regulation or more private-sector innovation. Support[edit] Many government officials and cybersecurity experts believe that the private sector has failed to solve the cybersecurity problem and that regulation is needed. Richard Clarke states that "industry only responds when you threaten regulation. If industry does not respond [to the threat], you have to follow through. Harris Miller, a lobbyist and president of the Information Technology Association of America , believes that regulation inhibits innovation. He states that "the private-sector must continue to be able to innovate and adapt in response to new attack methods in cyber space, and toward that end, we commend President Bush and the Congress for exercising regulatory restraint. Firms are just as concerned about regulation reducing profits as they are about regulation limiting their flexibility to solve the cybersecurity problem efficiently.

DOWNLOAD PDF WHAT REGULATIONS ARE NEEDED TO ENSURE AIR SECURITY?

Chapter 3 : The Basics of the Regulatory Process | Laws & Regulations | US EPA

What regulations are needed to ensure air security?: hearing before the Subcommittee on Energy Policy, Natural Resources, and Regulatory Affairs of the Committee on Government Reform, House of Representatives, One Hundred Seventh Congress, first session, November 27,

Each person who offers for transportation or transports a hazardous material shall ensure the package is properly labeled. There are a number of exceptions to the labeling requirements contained in Prohibited labeling is contained in The following is a list of additional requirements: Additional labeling Label Specifications Class 7 radioactive material There is a separate section for each of the authorized labels that gives an example of the label and describes the label. Each person who offers for transportation any hazardous materials subject to the HMR shall comply with the applicable placarding requirements. Applicability of placarding requirements Placarding is not required for infectious substances, ORM-D, limited quantities, small quantity shipments, and combustible liquids in non-bulk packages. Placards may not be displayed on any packaging, freight container, unit load device, motor vehicle or rail car unless the placard represents a hazardous material loaded into or onto the conveyance unless the shipment is in accordance with the TDG Regulation, the IMDG Code or the UN Recommendations. General placarding requirements are contained in Each bulk packaging, freight container, unit load device, transport vehicle, or rail car containing any quantity of hazardous materials must be placarded on each side and each end with the placards specified in Tables 1 and 2. When two or more Table 2 materials are contained in the same transport vehicle, the Dangerous" placard may be used instead of the specific placard required for each hazard class. However, when 1, kg 2, lbs. A frequent problem encountered involves the 1, lbs. Aggregate gross weight is the total weight of all hazardous materials and its packaging loaded on a single transport vehicle. For example, if a vehicle has 1, lbs. There are additional requirements for placarding such as: Placarding for subsidiary hazard Providing and affixing placards by Highway Visibility and display of placards Special placarding provisions by Highway General specifications for placards Providing and affixing placards by Rail There is a section for each placard that gives an example and describes it. For complete definition of hazmat employer and hazmat employee please see definitions contained in appendix A. All hazmat employees must have this training. This training provides information concerning the hazards posed by materials in the workplace and personal protection measures. The training may include basic emergency response procedures but is not intended to satisfy the requirements of 29 CFR Each hazmat employee must receive security awareness training. This training must include an awareness of security risks associated with hazardous materials transportation and methods designed to enhance transportation security. After March 25, , hazmat employees must receive this training at their next scheduled recurrent training, but in no case later than March 24, New hazmat employees must receive this training within 90 days of employment. In addition to the above security awareness training, hazmat employees of employers that are required to have a security plan must receive in-depth security training on the security plan and its implementation. The regulation does not specify sources of training. Training may be in any appropriate format including lecture, conference, self paced instruction, interactive video, etc. The record shall include: The records required by this rule must be produced upon reasonable demand by an authorized employee of the Department of Transportation. Records may be in any format such as paper or electronic files as long as they contain the required information and are readily available. Compliance with the current requirements for a CDL with a tank vehicle or hazardous materials endorsement provides a driver with the general knowledge and skills necessary to safely operate a commercial motor vehicle with hazardous materials cargo. This may satisfy the hazardous materials training requirements. As a hazmat employee, additional specialized training may be required based on the job function and material-specific requirements related to the handling of hazardous materials. The hazmat employer must determine the extent to which the CDL endorsement satisfies all training requirements. The number must be

maintained at all times that a shipment is in transit. The use of beepers, answering machines and switchboards is not authorized. The phone number must be to someone capable of providing information on the material. Written emergency response information must be appropriate for the hazardous material being transported. For transportation by highway, if a transport vehicle contains hazardous materials for which a shipping paper is required and the transport vehicle is separated from its motive power and parked at a location other than a facility operated by the consignee, consignor, or carrier, the carrier shall 1 Mark the transport vehicle with the telephone number of the motor carrier on the front exterior near the brake hose or electrical connection; or 2 have the shipping paper and emergency response information readily available on the transport vehicle. This requirement does not apply if the identification number for each hazardous materials contained therein is marked on the outside of the vehicle on an orange panel or white square on point placard. The employer is also required to train their hazmat employees on the security plan. The purpose of these requirements is to enhance the security of hazardous materials transported in commerce. Each person who offers for transportation in commerce or transports in commerce one or more of the following hazardous materials must develop and adhere to a transportation security plan for hazardous materials that conforms to the requirements of this subpart. As used in this section, "large bulk quantity" refers to a quantity greater than 3, kg 6, pounds for solids or 3, liters gallons for liquids and gases in a single packaging such as a cargo tank motor vehicle, portable tank, tank car, or other bulk container. Any quantity of a Division 1. Conducted by highway or rail; In direct support of their farming operations; and Conducted within a mile radius of those operations. It is a packaging construction system based on performance standards developed in the form of Recommendations by the United Nations Committee of Experts on the Transport of Dangerous Goods UN Recommendations. The UN standards have general requirements for materials, construction and a maximum capacity. Containers must pass or be capable of passing a series of performance tests before they are authorized for the carriage of hazardous materials. The international standards have general requirements for materials, construction and a maximum capacity as compared to detailed DOT specifications for non-bulk packagings formerly contained in 49 CFR, Part Packaging requirements are based on the Packing Group of the material, its vapor pressure, and chemical compatibility between the package and the HM. Non-bulk packaging standards are based upon a number of performance tests. In addition to UN Recommendation performance oriented tests, a vibration test for non-bulk packaging is required domestically. Reuse of plastic and metal is drums based on minimum thickness requirements. This substitutes for the lack of performance tests in UN standards with regard to puncture resistance, abrasion resistance and metal fatigue. Package manufacturers must provide written notification to customers of any specification shortfalls or steps to be taken to conform with applicable specification. Performance tests for UN packaging, including design qualification tests and periodic retests, are included in Part Packing Groups The packing group designated in the The shipper is responsible for determining the appropriate packing group.

Chapter 4 : 49 U.S. Code Â§ - Air transportation security | US Law | LII / Legal Information Institute

In their different guises they can be found in civil airspace or flying as integral players in military missions. Accordingly, ISO and DO could prove helpful in perpetuating safety and security for unmanned systems. Software tools that automate the processes required by these certification standards are easing the burden. The major difference between UAVs and the toys of our childhood is the sophistication of the vehicles themselves and of their navigation and pilot systems. Given that these vehicles enter civil airspace and will continue to do so more and more as they begin to be used for an increasing number of civilian activities, the safety and security of UAV software has become critical. And, with no mandated standards in place to govern the safety and security of UAV systems, the proliferation of drones increases the overall risk to our safety and security. Notably, even if FAA standards are imposed, safety might still be at risk unless security standards are mandated. The crash of a CIA drone in Iran underlines that unless a system can withstand hacking, safety remains at risk. In that incident, local authorities claimed that they had diverted the vehicle by hacking its GPS. Department of Homeland Security. The team spoofed an onboard GPS receiver by mimicking the actual signals sent to the global positioning device to trick the UAV into following different commands. To address such a scenario, developers at the U. Air Force Institute of Technology are working on a system that enables a UAV, like a human pilot, to supplement GPS navigation with visual feedback by using a camera with pattern-recognition software. Such efforts are only as secure as the security of the software deployed. Safety is clearly important in UAV development, but a UAV can only be considered safe if it cannot be controlled by a hostile intruder. Security functional requirements include audit, communications, cryptography, data protection, authentication, security management, privacy, and protection of Targets of Evaluation TOEs. Click graphic to zoom by 1. Each software level has associated objectives that must be satisfied during development. DO defines a range of software levels that must be examined and determined for each software component. To help developers do this, the standard outlines needed processes such as requirements traceability, software design, coding, and the validation and verification that ensure confidence in and the correctness and control of the software. Robust software validation and verification processes enable developers to detect and correct errors introduced during software development. With respect to software, the overlap between the two standards is considerable, especially with configuration management, software development, quality assurance, verification, and planning. However, DO focuses solely on the safety of the software in the airborne system, while ISO focuses on system security. These language subsets consist primarily of lists of constructs and practices for developers to avoid in order to ensure safe or secure code. Given the anticipation that UAVs will fall under both DO and ISO standards, development teams should strive to fulfill the aims of both standards moving forward. It is certainly critical to ensure that the UAV is developed to meet system requirements that ensure safety and security issues are dealt with. However, with increasing market pressure related to UAV development, improvements in time-to-market and development costs are also important. Meeting one standard is a challenge; adhering to two such as DO and ISO is totally daunting. By applying appropriate automation techniques, development teams can minimize the overhead involved. To help manage this matrix of relationships, requirements-traceability tools link system requirements to software requirements, from the software requirements to design artifacts, and then to source code and the associated test cases. The automated bidirectional tracing of requirements ensures that the developed UAV does exactly what is specified by the final set of requirements â€" no more, no less, and no matter how often those requirements change Figure 2. Requirements traceability is a vital factor in meeting security and safety standards. Dynamically linking high-level requirements to source code and verification tasks ensures that an up-to-date traceability matrix is always maintained. Again, the rules designed to develop safe code are similar to those

designed for secure code. Static analysis automates verification of coding rules. Once the rules are selected, the source code is statically analyzed to highlight the precise location of any rule violations. Static analysis helps to fulfill other obligations too. For example, it identifies code that is unnecessarily complex and therefore more error prone. Developers must prove not only that the code functions correctly, but that all code is exercised to a degree appropriate to the criticality of the system. Dynamic analysis tools Dynamic analysis tools exercise code as a whole system or piecemeal, by means of unit or integration testing, to show correct functionality. Any code necessary to permit a subsystem to be built and executed is created automatically, and the exercised code is identified. Even if they were, those standards do not insist either on the use of automated tools or on the automation of the development process. However, the need for UAVs to be safe and secure is vital given their expanded role. Automated requirements traceability coupled with modern static- and dynamic-analysis tools make it viable to meet the exacting demands of such standards in an efficient and cost-effective manner. He can be contacted at Mark.

Chapter 5 : Security Regulations

The BiblioGov Project is an effort to expand awareness of the public documents and records of the U.S. Government via print publications. In broadening the public understanding of government and its work, an enlightened democracy can grow and prosper.

Chapter 6 : Full text of "WHAT REGULATIONS ARE NEEDED TO ENSURE AIR SECURITY?"

To ensure congressional and public input into the regulatory deci- sionmaking process, this subcommittee held a November 27, , hearing entitled, "What Regulations are Needed to Ensure Air Se-.

Chapter 7 : IAC Air Cargo Security Training FAQs

The security laws, regulations and guidelines directory Need to find and understand security and privacy laws, regulations and guidelines? Here's a handy compendium with summaries plus links to.